The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
10/04/2019

SUBJECT:
Multiple Vulnerabilities in Cisco Products Could Allow for Arbitrary Code Execution With Root Privileges

OVERVIEW:
Multiple vulnerabilities have been discovered in Cisco products, the most severe of which could allow for arbitrary code execution with root privileges on the affected system. An attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- Adaptive Security Virtual Appliance (ASAv)
- Cisco FMC Software.
- Cisco products if they are running a vulnerable release of Cisco ASA Software or Cisco FTD Software that is configured to perform FTP inspection.
- Cisco products that are running a vulnerable release of Cisco ASA Software and that have either the Clientless SSL VPN or AnyConnect SSL VPN enabled.
- Cisco products that are running a vulnerable release of Cisco ASA Software or Cisco FTD Software that is configured to support OSPF routing.
- Firepower 2100 Series Appliances
- Firepower 4100 Series Security Appliances
- Firepower 9300 Series Security Appliances
- Firepower Threat Defense Virtual (FTDv)

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home Users: Low

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in Cisco products, the most severe of which could allow for arbitrary code execution with root privileges on the affected system. Details of these vulnerabilities are as follows:

- A vulnerability in the FTP inspection engine of Cisco Adaptive Security (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated remote attacker to cause a denial of service (DoS) condition on an affected device. (CVE-2019-12673)
- A vulnerability in the Internet Key Exchange version 1 (IKEv1) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated remote attacker to trigger a reload of an affected device resulting in a denial of service (DoS) condition. (CVE-2019-15256)
- A vulnerability in the Open Shortest Path First (OSPF) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated adjacent attacker to cause a reload of an affected device resulting in a denial of service (DoS) condition. (CVE-2019-12676)
- A vulnerability in the Session Initiation Protocol (SIP) inspection module of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated remote attacker to cause a denial of service (DoS) condition on an affected device. (CVE-2019-12678)
- A vulnerability in the Secure Sockets Layer (SSL) VPN feature of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated remote attacker to cause a denial of service (DoS) condition that prevents the creation of new SSL/Transport Layer Security (TLS) connections to an affected device. (CVE-2019-12677)
- A vulnerability in the web UI of the Cisco Firepower Management Center (FMC) could allow an authenticated remote attacker to inject arbitrary commands that are executed with the privileges of the root user of the underlying operating system. (CVE-2019-12690)
- A vulnerability in the web UI of the Cisco Firepower Management Center (FMC) could allow an authenticated remote attacker to execute arbitrary commands on an affected device. (CVE-2019-12687, CVE-2019-12688)
- A vulnerability in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated remote attacker to execute arbitrary code on the underlying operating system of an affected device. (CVE-2019-12689)
- Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated remote attacker to execute arbitrary SQL injections on an affected device. (CVE-2019-12679, CVE-2019-12680, CVE-2019-12681, CVE-2019-12682, CVE-2019-12683, CVE-2019-12684, CVE-2019-12685, CVE-2019-12686)
- Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. (CVE-2019-12674, CVE-2019-12675)

Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution with root privileges on the affected system. An attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMENDATIONS:

The following actions should be taken:

- Install the update provided by Cisco immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

Cisco:

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-asa-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-asa-ftd-ikev1-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-asa-ospf-lsa-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-asa-ftd-sip-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-asa-ssl-vpn-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-fmc-com-inj
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-fmc-rce
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-fmc-rce-12689
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-fmc-sql-inj
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-ftd-container-esc

CVE:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12673
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12674
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12675
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12676
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12677
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12678
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12679
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12680
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12681
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12682
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12683
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12684
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12685
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12686
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12687

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12688
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12690
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-15256

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

Chris Watts
Security Operations Analyst
MS Department of Information Technology Services
601-432-8201 | www.its.ms.gov

ITS Mississippi Department of Information Technology Services
3771 Eastwood Drive | Jackson, Mississippi 39211-6381

DISCLAIMER: This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager. This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited